Department of Homeland Security
Information Analysis and Infrastructure Protection
Daily Open Source Infrastructure Report for 16 October 2003

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
www.whitehouse.gov/homeland

Daily Overview

- Microsoft has released "Security Bulletin MS03−041: Vulnerability in Authenticode Verification Could Allow Remote Code Execution (Critical)" and a patch is available on the Microsoft Website. (See item 25)
- Microsoft has released "Security Bulletin MS03−042: Buffer Overflow in Windows Troubleshooter ActiveX (Critical)" and a patch is available on the Microsoft Website. (See item 26)
- Microsoft has released "Security Bulletin MS03−043: Buffer Overrun in Messenger Service Could Allow Code Execution (Critical)" and a patch is available on the Microsoft Website. (See item 27)
- Microsoft has released "Security Bulletin MS03−044: Buffer Overrun in Windows Help and Support Center Could Lead to System Compromise (Critical)" and a patch is available on the Microsoft Website. (See item 28)
- Microsoft has released "Security Bulletin MS03−046: Vulnerability in Exchange Server Could Allow Arbitrary Code Execution (Critical)" and a patch is available on the Microsoft Website. (See item 30)
- SecurityFocus has raised ThreatCon to Level 2, citing a need for increased vigilance.
- Internet Security Systems has raised Alertcon to Level 2, citing a need for increased vigilance.

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical; Defense Industrial Base
Service Industries: Banking and Finance; Transportation; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information and Telecommunications; Internet Alert Dashboard
Other: General; DHS/IAIP Web Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *October 15, The Courier−Journal (KY)* — **Natural gas pipeline explodes near French Lick, Indiana.** An explosion of a gas pipeline in Orange County, IN, forced a state highway to be closed Tuesday, October 14, and a few homes to be briefly evacuated. The explosion occurred on the property of the Texas Eastern Natural Gas compressor station outside French Lick at 1:22 p.m. Damage was confined to the pipeline within the grounds of the facility, according to the Orange County Sheriff's Department and a spokesperson for Houston−based Texas Eastern. An on−site company crew "immediately shut down that section of the pipeline," said Texas Eastern spokeperson Gretchen Krueger. "There was no ignition of the line, (and) there was no danger to the surrounding area" Krueger said. **The cause of the pipeline rupture is under investigation. Krueger said the pipeline is part of a system that runs between the Texas Gulf Coast and New York City. It supplies natural gas to local companies along the way that in turn deliver the gas to homes and businesses.** "There was minimal or no impact" on the customer gas companies, Krueger said.
   Source: http://www.courier−journal.com/localnews/2003/10/15ky/met−4− gas1015−2577.html

2. *October 15, The Plain Dealer (OH)* — **Bottom of reactor found to be leak−free. There are no leaks in the bottom of the Davis−Besse nuclear reactor in Ohio, engineers concluded Tuesday, October 14, after completing an exhaustive analysis of digital photographs taken by a robotic camera.** "We see no leaks at all," said Lew Myers, chief operating officer of plant owner FirstEnergy's nuclear operating company. Nuclear Regulatory Commission (NRC) spokesperson Jan Strasma confirmed the finding. Though NRC inspectors paid special attention to the photographic analysis, the company must still submit its final reports to the agency, said Myers. The special NRC panel overseeing FirstEnergy's rehabilitation of the power plant must sign off. **Before getting permission to restart the reactor before year's end, the company must still modify emergency cooling pumps that could clog after an accident.** More importantly, the NRC has made it clear that before it can allow the reactor to be restarted, FirstEnergy must prove it has reformed its management practices. That behavior, the company itself said, put safety behind profits and allowed managers to ignore safety issues that employees brought up.
   Source: http://www.cleveland.com/news/plaindealer/index.ssf?/base/news/106621034545820.xml

[Return to top]

Chemical Sector

3. *October 15, The Times−Picayune (LA)* — **Group is urging oil refineries to stop using deadly chemical.** A national public advocacy group has called on oil refineries, including five in Louisiana, to stop using hydrofluoric acid, a deadly chemical that puts nearby communities at risk in the event of a leak. **In a report called "Needless Risk" issued Tuesday, the U.S.**

Public Interest Research Group said the threat of a catastrophic terrorist attack should force chemical plants and refineries to rethink how safe their facilities are. It said current defenses against a leak are inadequate. A release in 1987 from a refinery in Texas City, Texas, sent 1,000 people to the hospital and forced 3,000 people from their homes for three days. **With eleven refineries using HF, Texas leads the nation, followed by Louisiana with five−−including four in the metropolitan New Orleans area storing nearly 2.5 million pounds of the chemical, according to the Environmental Protection Agency.** The Louisiana facilities are Exxon Mobil's refinery in Chalmette, Murphy Oil in Meraux, ConocoPhillips refining in Belle Chasse, Marathon Ashland Petroleum in Garyville and Placid Refining in Port Allen near Baton Rouge.
Source: http://www.nola.com/news/t−p/index.ssf?/base/news−0/10661973 45101260.xml

[Return to top]

Defense Industrial Base Sector

4. *October 15, Associated Press* — **NATO launches new, modern strike force.** NATO launched its elite rapid−reaction force Wednesday, October 15. The NATO Response Force's initial core of 9,000 troops, backed by naval and air power, was inaugurated during a ceremony at NATO's northern command. **The full force is to become fully operational in October 2006 with 20,000 troops able to deploy within five to 30 days to deal with operations ranging from evacuations and peacekeeping to counterterrorism or high−intensity combat**. The new force will not be a standing unit, but rather a pool of elite troops trained to work together and ready to respond immediately to a NATO mobilization order. Units from national forces will move in and out of the force in six−month rotations.
Source: http://www.nytimes.com/aponline/international/AP−NATO−Respon se−Force.html

5. *October 14, Global Security Newswire* — **Army claims perfect missile interception record in Iraq war. The Army has formally concluded that it successfully shot down every Iraqi ballistic missile it tried to intercept during combat this year, but officials have decided to delay releasing the information used to reach that conclusion.** "In almost all cases, there is scientific data that shows [the intercepts]," said Lt. Gen. Joseph Cosumano, who heads the Army Space and Missile Defense Command. "You can almost see the breakup" of the Iraqi missiles, he said. Sparking controversy following the 1991 Gulf War, senior U.S. officials cited high Patriot success rates during that war, but later analyses suggested that far fewer Patriots actually intercepted their targets or killed the warheads. **"We took the lessons learned from Desert Storm [and] put the data recording capabilities in those weapons systems," said Brig. Gen. John Urias,** deputy commanding general for acquisition of the Army Space and Missile Defense Command.
Source: http://www.govexec.com/dailyfed/1003/101403gsn1.htm

[Return to top]

Banking and Finance Sector

6.

October 15, The Philadelphia Inquirer — **Man enters guilty plea in credit card 'cloning' scam. A Tunisian national on Tuesday, October 14, admitted his role in a sophisticated counterfeiting scheme in which he "cloned" hundreds of credit cards at the Philadelphia, PA, bar where he worked and then reproduced them in a makeshift shop in his apartment.** Faker Bensalem pleaded guilty in federal court to charges of conspiracy, counterfeiting and immigration fraud in a scheme that prosecutors say victimized 271 people nationwide, 47 financial institutions and caused losses totaling $108,000. Bensalem and another Tunisian national, Anis Kalthoumi were arrested by authorities in a scheme in which they used a palm−sized scanning device that reads the credit information in the magnetic strip on credit cards. Bensalem then downloaded the data onto his home computer and used a device to transfer the data onto the magnetic strip on blank credit cards. Prosecutors said he then used an embosser to imprint the raised lettering on the counterfeits.
Source: http://www.philly.com/mld/inquirer/news/local/7014740.htm

7. *October 15, Associated Press* — **Florida launches program to help identity theft victims.** The State of Florida launched a program Wednesday, October 15, aimed at curtailing identity theft and help its victims restore their good credit and reputations. **The attorney general's office set up a Website that provides information to help people report identity theft, clean their credit records and clear their names of crimes they did not commit. It also gives tips on how to prevent identity theft.** In addition, the Florida Department of Law Enforcement will now issue a document, called "Compromised Identity Certificate," designed to help victims prove to potential employers, landlords or others that they did not commit crimes that wrongly show up in background checks.
Source: http://www.miami.com/mld/miamiherald/business/7020514.htm

[Return to top]

Transportation Sector

8. *October 15, Associated Press* — **Labor unrest roils Southern California. Labor disputes in Southern California, left hundreds of thousands of commuters stranded, grocery shoppers inconvenienced, and county jails and courts threatened with closure. The strike by the Metropolitan Transportation Authority entered its second day Wednesday, stalling the nation's third−largest mass−transit system.** Some 2,000 MTA mechanics walked out, with an additional 6,000 bus drivers and clerks honoring their picket lines. Meanwhile, 70,000 grocery clerks from three chains −− Kroger Co.'s Ralphs, Safeway Inc.'s Vons and Albertsons Inc. −− began their fourth day on the picket lines in Southern and Central California on Wednesday with no sign of a new contract. **In another dispute, 219 out of the 343 Los Angeles County sheriff's deputies who provide security at jails called in sick Wednesday morning to protest stalled labor talks,** said deputy Bill Spear, a sheriff's spokesman. The deputies have had sporadic sickouts over the past three weeks, forcing officials to curtail some court activities. Jack Kyser, chief economist for the Los Angeles Economic Development Corp., estimated the transit strike could cost $4 million a day while the toll from the supermarket walkout could reach $6.3 million a day in lost wages. **"Those in both disputes are digging in their heels. And the common thread here is health benefits," Kyser said.**
Source: http://www.newsday.com/news/nationworld/nation/sns−ap−california−strikes,0,7231343.story?coll=ny−nationalnews−headlines

9. *October 15, U.S. Newswire* — **TSA demonstrates new bus security measures.** On Wednesday, Transportation Security Administration (TSA), key members of Congress, and Greyhound Lines, Inc. came together to demonstrate some of the latest advancements in security for the tens of millions of Americans who travel on intercity buses every year. **The star of the day was Greyhound's bus 7211, which has been outfitted with a driver protection shield and state−of−the−art tracking and telecommunications equipment. The clear plastic driver shield presents a significant obstacle to any passenger that might want to do harm to the bus operator and gives the driver valuable time to bring the bus to a stop before responding to a situation.** Meanwhile, the Global Positioning System and wireless telecommunications allow the driver to immediately alert authorities to an incident and rapidly transmit the bus' position anywhere in the country. This allows police to quickly respond to resolve any incident and gives fire and paramedics units a head start in finding and treating potential victims. **These security upgrades are a few of the numerous initiatives TSA is helping to fund with $20 million in grants announced August 5, 2003.** The grants fund 67 projects proposed by bus companies and others located in 25 states and the District of Columbia.
Source: http://releases.usnewswire.com/GetRelease.asp?id=118−1015200 3

10. *October 15, Associated Press* — **Police search for laptop with airport−screening information.** An instructor teaching a group of new airport security screeners had his laptop stolen after leaving it in a hotel meeting room during a break in the seminar, officials said. The theft occurred between noon and 12:30 p.m. Tuesday at the Embassy Suites Hotel near Philadelphia International Airport, authorities said. **The laptop contains sensitive−−but not highly classified−−material**, a Transportation Security Administration (TSA) official said. The files outlined standard airport screening procedures such as the use of magnetometers, which anyone visiting an airport could view. "It is not any kind of reverse road map to penetrate the security system," TSA spokesman Mark Hatfield said Wednesday, a day after the apparent theft. "Nonetheless, **it's not something that we're interested in seeing proliferated or distributed publicly**." Both local police and federal investigators, including some from the FBI, were working on the case.
Source: http://pennlive.com/newsflash/pa/index.ssf?/base/news−8/1066 240747314621.xml

11. *October 15, Business Wire* — **Amtrak's Capitol Corridor launches Wi−Fi trial on rail cars. Capitol Corridor Joint Powers Authority (CCJPA) has announced a three−month "Wi−Fi" or wireless fidelity trial for Amtrak's Capitol Corridor intercity train service, operating between the Sierra foothills, Sacramento, Oakland/San Francisco and San Jose, California.** Wireless Internet connectivity will be available along the 170−mile rail corridor for passengers wishing to work, communicate and be entertained while traveling. **Amtrak's Capitol Corridor is the first U.S. intercity rail operator to offer Wi−Fi as a differentiated onboard service.** Passengers only need a Wi−Fi−enabled laptop computer or PDA to access the broadband wireless service. The pilot program provides an opportunity for Amtrak's Capitol Corridor to better serve the community of business and leisure travelers in the corridor.
Source: http://home.businesswire.com/portal/site/google/index.jsp?ndmViewId=news_view&newsId=20031015005389&newsLang=en

12.

October 15, Associated Press — **Injuries reported in New York ferry accident. A Staten Island ferry slammed into a pier as it was docking Wednesday afternoon, and a police source said at least a dozen people were feared dead.** The crash tore off victims' limbs, and passengers jumped for their lives from the shattered vessel as the accident ended an otherwise routine trip to Staten Island from lower Manhattan. Other commuters were trapped in piles of debris aboard the 22−year−old ferry. **The cause of the accident was not immediately known. The 300−foot vessel slammed into the wooden pilings along the side of a dock as it arrived on the Staten Island end of its run across New York Harbor just before the start of the evening rush,** said Fire Department spokesman Mike Loughran. The ship sustained a huge hole in its side, officials said. **The ferry, which has three levels, has a capacity of 6,000. It was not immediately clear how many people were aboard at the time.** The Staten Island Ferry carries 70,000 commuters a day on the 25−minute free ride between Staten Island and lower Manhattan. Five boats make 104 daily trips between the two boroughs.
Source: http://www.washingtonpost.com/wp−dyn/articles/A30748−2003Oct 15.html

13. *October 14, Government Executive Magazine* — **Airport industry presses TSA for guidance on using private screeners.** The Transportation Security Administration (TSA) should provide airport managers with guidance on using private screeners as soon as possible so they can begin planning before a federal deadline next year, an airport industry representative said Tuesday. **TSA awarded the first phase of a contract last week to evaluate the performance of private screening companies at airports in Kansas City, MO; San Francisco; Rochester, NY; Tupelo, MS; and Jackson Hole, WY. The airports are part of a pilot program to compare the effectiveness and service of private screeners against federal workers at 436 airports under the jurisdiction of TSA.** When TSA was created almost two years ago, Congress stipulated that airports must use federal workers to screen passengers and baggage for weapons and explosives, except at the five airports in the pilot program. However, legislators included a provision that permits airports to opt out of the federal program and hire private screeners starting in November 2004.
Source: http://www.govexec.com/dailyfed/1002/101403c1.htm

[Return to top]

Postal and Shipping Sector

14. *October 15, DM News* — **USPS expects rising volume.** The U.S. Postal Service (USPS) is ready to handle an expected increase in volume during the fall season due to a rebounding economy and improvements to its own processes and those of mailers, a postal official said. "The system is running well right now, and we do not anticipate any problems," said Paul Vogel, vice president of network operations management at the USPS. **"We are predicting that there is going to be a 2 percent increase in Standard Mail volume this season over last year.** This is primarily driven by the improvements in the economy." The USPS also is meeting most of its in−home delivery dates, Vogel said. **One reason for the agency's improved performance this year is that more businesses are using printers, consolidators and other USPS partners to prepare mail and receive drop−ship discounts.** For mail that is not presorted, the USPS is relying heavily on 529 automated flat−sorting machines. During last year's busy fall season, the USPS "was at the tail end of the deployment of these machines, so people may not have been as proficient with using them," Vogel said. "But this year, we have a

full year experience under our belt."
Source: http://www.dmnews.com/cgi−bin/artprevbot.cgi?article_id=2527 6

15. *October 14, Government Executive Magazine* — **Postal workers sue over anthrax exposure. A group of Washington, DC area Postal Service employees who claim they were deliberately left in harm's way during the 2001 anthrax attacks plan to file a class action suit Wednesday against the agency.** Brentwood Exposed, a group professing to represent hundreds of current and former postal workers, allege that U.S. Postal Service leaders violated the employees' Fifth Amendment rights by withholding information relating to contamination at the Joseph Curseen Jr. and Thomas Morris Jr. Processing and Distribution Center, formerly known as the Brentwood Mail Processing and Distribution Center. **Postal executives have said they took their cues from the U.S. Centers for Disease Control and Prevention (CDC). It wasn't until the CDC confirmed contamination that the facility was shut down.**
Source: http://www.govexec.com/dailyfed/1003/101403w1.htm

[Return to top]

Agriculture Sector

16. *October 15, USAgNet* — **New Zealand hit by hog disease. An outbreak of a hog disease that cannot be treated has hit New Zealand. Agriculture officials, citing initial tests at a pig farm where a third of the piglets died, said final DNA results won't be available for two weeks, but other clinical and pathological tests showed the animals had post−weaning multisystemic wasting syndrome.** Ministry of Agriculture and Forestry exotic disease response coordinator The disease causes the animals to waste away and is connected with other pig viruses such as porcine parvovirus. The disease was identified in the early 1990s and has since been found with increasing frequency in pig farms in the U.S., Canada, Europe, and Asia. **Until now, New Zealand and Australia have been among the few countries that had no cases.**
Source: http://www.usagnet.com/story−national.cfm?Id=1112&yr=2003

[Return to top]

Food Sector

17. *October 15, Agricultural Research Service* — **Automatic poultry inspection goes on line. The Automatic Poultry Inspection System developed by Agricultural Research Service (ARS) scientists is ready for its first long−term testing in commercial processing plants, having just successfully passed a four−day test in a commercial broiler−processing plant.** For the four−day test, Yud−Ren Chen, an agricultural engineer at the ARS, and colleagues took their inspection equipment to a commercial processing facility. **The Automatic Poultry Inspection System had an accuracy rate of 92 to 95 percent. ARS has a cooperative research and development agreement to commercialize Chen's system and move it into use among the nation's 300−plus poultry processing plants.** The system quickly diagnoses all physical or nonmicrobial, biological conditions that cause an inspector to remove a chicken from the processing line. In Chen's system, when a chicken carcass passes through a light beam,

the interruption triggers a scan with a light probe from about an inch away. The reflected light is analyzed by a computer using ARS−developed "Automated Poultry Inspector" software to identify variations in external skin color and texture and tissue composition, which are clues to problems.
Source: http://www.ars.usda.gov/is/pr/2003/031015.htm

[Return to top]

Water Sector

18. *October 15, Oregonian* — **Cities closing open water reservoirs. Only 16 large U.S. utilities have open drinking water reservoirs. And at least half intend to bury or cover them to improve water security.** But proposed federal rules would not require Portland, OR, to cover or bury the reservoirs. The pending rules give the city the option of trying to keep the reservoirs open with less than the 50 to 100 foot exclusion zones. Portland's reservoir burial, approved last year by the City Council, has triggered opposition. Opponents of burial want the city to reconsider the decision. To keep the reservoirs uncovered the city would have to go against the advice of two security consultants who said that the reservoirs might be successfully attacked. Rosemary Menard, the bureau's director of water resources management, said the city could pursue a slimmed−down risk mitigation plan. But she said the bureau can't pursue that option in good conscience given the security concerns. **The Environmental Protection Agency's proposed regulations would require any city that wants to maintain its open reservoirs to get a state approved risk mitigation plan. The plan would be required to address physical access.** "If you look nationally, one way or another they're eventually going to get everybody with some rule or another," said Martin Adams, director of water quality and operations for the Los Angeles Department of Water and Power.
Source: http://www.oregonlive.com/news/oregonian/index.ssf?/base/news/106621943125920.xml

19. *October 15, Tampa Tribune* — **Water system security plans, maps stolen.** Officials reassured the public about the safety of Tampa, Florida's water supply Tuesday after someone stole maps and instructions related to water−treatment−plant security systems from a consultant's truck. The consultant was hired to help with security enhancements at the Tampa Water Department, officials said. **A binder containing maps of Tampa's water treatment plants, instructions on their security cameras and defense systems, and two manuals with instructions on the wiring of their control panels was stolen**, police said. None of those planned improvements has been implemented, water department officials said. **"The material that was taken does not compromise the security of the water department in any way," said Major Jane Castor, the Tampa police homeland security liaison.** "Even if it fell into the wrong hands, it's not something that can't be overcome." As a precaution, police will increase patrols near the dam and the water transfer system, Castor said.
Source: http://news.tbo.com/news/MGAL96PSSLD.html

[Return to top]

Public Health Sector

20. *October 15, Toledo Blade* — **Measure lets health agency hide information during investigations. The Ohio Department of Health would be able to conceal information from the public during an investigation into the cause of any disease or illness under a bill that a state Senate committee approved Tuesday. The bill that would give the state more power to combat a potential bioterrorism attack also would give businesses the same privacy as citizens while the state health department conducts an investigation**. It does so by allowing the public to receive information about pending investigations if it is in "summary, statistical, or aggregate form and ... does not identify a person." In addition to an individual, the word "person" in the Ohio Revised Code is interpreted to cover a business or a corporation. Currently, the state can conceal information during an investigation that would identify an individual. Jodi Govern, general counsel of the state health department, said the change in state law would give the department the same confidentiality for its investigations that law enforcement now has. The bill would enable the public to get access to information from investigations after they are completed, and would authorize release of limited information every six months on pending investigations.
Source: http://www.toledoblade.com/apps/pbcs.dll/article?AID=/20031015/NEWS24/110150098

21. *October 15, USA Today* — **Sports teams warned about skin infection. Concern is growing within the sports world over a bacterial infection resistant to antibiotics that flourishes in a sports environment.** Recent cases on high school, college, and professional football teams have been reported nationwide. According to the U.S. Centers for Disease Control and Prevention (CDC), the bacteria is spread in ways that come with the territory in sports, including contact with infected persons or by contact with shared towels or equipment that carry the bacteria. **In August, the medical and training staffs of every National Football League club were sent copies of a CDC report about infections in sports related to the bacteria called methicillin−resistant staphylococcus aureus (MRSA). On Monday, the National Collegiate Athletic Association issued an "alert on skin infections" to schools. The National Federation of High School Associations says it will send a similar alert this week to high school sports bodies.** Cases had been associated with patients in hospitals. "Now we're seeing it emerge in settings where people have little or no contact with health care and are generally healthy, sports teams are just the last couple of years," says Jeff Hageman, an epidemiologist with the CDC.
Source: http://www.usatoday.com/news/nation/2003−10−14−sports−infect ions_x.htm

[Return to top]

Government Sector

22. *October 14, National Journal's Technology Daily* — **Homeland Security issues interim rule on industry liability.** The Homeland Security Department on Tuesday announced an interim rule designed to limit the liability risks associated with anti−terrorism technology. The announcement came during a seminar with industry officials. **"It is in the public's interest to have this interim rule effective immediately because its aim is to foster the development and deployment of anti−terrorism technologies," said the rule signed by Homeland Security Secretary Tom Ridge** late on Friday. The regulation also seeks to clarify the process

for seeking protection under the law in order to provide "an instant incentive for prospective applicants ... and for others to begin exploring new measures that will prevent or reduce acts of terrorism." **Industry officials who attended the seminar agreed that an urgent need exists for manufacturers to apply for the liability protections under the statute, which was enacted in January.** Liability protects companies if their anti−terrorism products fail to prevent attacks. The interim regulation would let manufacturers retain liability for five to eight years.
Source: http://www.govexec.com/dailyfed/1003/101403td1.htm

[Return to top]

Emergency Services Sector

23. *October 15, Federal Computer Week* — **Cox proposes faster funding for responders.** Rep. Christopher Cox (R−CA), chairman of the House Select Committee on Homeland Security, last week introduced a bill that would streamline and expedite what critics describe as a cumbersome process for getting homeland security funds to first responders. **H.R. 3266 −− also called the Faster and Smarter Funding For First Responders Act −− essentially would reduce a 12−step grant, reducing the process to two steps. It would allow states and regions to apply for grants, which would be awarded based on the greatest threat to an area rather than a population−based formula.** More than a month ago, Cox and other government officials and homeland security experts complained that the grant process was fragmented and the formulas were "complicated and eccentric" because they were built for political needs. **Under the bill, funds could be used for buying new or upgrading existing equipment and training on it, as well as training and exercises related to prevention and emergency preparedness.**
Source: http://www.fcw.com/geb/articles/2003/1013/web−cox−10−14−03.a sp

24. *October 15, Government Technology* — **Virginia makes real−time traffic camera images available to first responders .** The Virginia Department of Transportation (VDOT) is making its traffic camera images available to first responders so they can have access to real−time images when responding to emergencies. **"First responders want to see what our eyes are seeing through the 75 traffic cameras located along major interstates in Northern Virginia,"** said Kevin Barron, VDOT's program manager for intelligent transportation systems (ITS).
Source: http://www.govtech.net/news/news.php?id=2003.10.15−72972

[Return to top]

Information and Telecommunications Sector

25. *October 15, Microsoft* — **Microsoft Security Bulletin MS03−041: Vulnerability in Authenticode Verification Could Allow Remote Code Execution. A vulnerability in Authenticode could, under certain low memory conditions, allow an ActiveX control to download and install without presenting the user with an approval dialog**. To exploit this vulnerability, an attacker could host a malicious Website. If a user then visited that site an

ActiveX control could be installed and executed on the user's system. An attacker could also send an HTML e−mail to the user. If the user viewed the HTML e−mail an unauthorized ActiveX control could be installed and executed on the user's system. Exploiting the vulnerability would allow the attacker only the same privileges as the user. **Microsoft has assigned a risk rating of "Critical" to this issue** and recommends that system administrators install the patch immediately.
Source: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03−041.asp

26. *October 15, Microsoft* — **Microsoft Security Bulletin MS03−042: Buffer Overflow in Windows Troubleshooter ActiveX Control Could Allow Code Execution. Microsoft's Local Troubleshooter ActiveX control (Tshoot.ocx) contains a buffer overflow that could allow an attacker to run code of their choice on a user's system in the context of the user**. Because this control is marked "safe for scripting", an attacker could exploit this vulnerability by convincing a user to view a specially crafted HTML page that references this ActiveX control. To exploit this vulnerability, the attacker would have to create a specially formed HTML−based e−mail and send it to the user. Alternatively an attacker would have to host a malicious Web site that contained a Web page designed to exploit this vulnerability. **Microsoft has assigned a risk rating of "Critical" to this issue** and recommends that system administrators install the patch immediately.
Source: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03−042.asp

27. *October 15, Microsoft* — **Microsoft Security Bulletin MS03−043: Buffer Overrun in Messenger Service Could Allow Code Execution. A vulnerability in the Messenger Service results because the Service does not properly validate the length of a message before passing it to the allocated buffer**. An attacker who successfully exploited this vulnerability could be able to run code with Local System privileges on an affected system, or could cause the Messenger Service to fail. The attacker could then take any action on the system, including installing programs, viewing, changing or deleting data, or creating new accounts with full privileges. If users have blocked the NetBIOS ports (ports 137−139) − and UDP broadcast packets using a firewall, others will not be able to send messages to them on those ports. Disabling the Messenger Service will prevent the possibility of attack. **Microsoft has assigned a risk rating of "Critical" to this issue and recommends that system administrators disable the Messenger Service immediately and evaluate their need to deploy the patch**.
Source: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03−043.asp

28. *October 15, Microsoft* — **Microsoft Security Bulletin MS03−044: Buffer Overrun in Windows Help and Support Center Could Lead to System Compromise. A security vulnerability in the Help and Support Center function which ships with Windows XP and Windows Server 2003 results because a file associated with the HCP protocol contains an unchecked buffer**. An attacker could exploit the vulnerability by constructing a URL that, when clicked on by the user, could execute code of the attacker's choice in the Local Computer security context. The URL could be hosted on a web page, or sent directly to the user in email. In the Web based scenario, where a user then clicked on the URL hosted on a website, an attacker could have the ability to read or launch files already present on the local machine. The

affected code is also included in all other supported Windows operating systems, although no known attack vector has been identified at this time because the HCP protocol is not supported on those platforms. **Microsoft has assigned a risk rating of "Critical" to this issue** and recommends that system administrators install the patch immediately.
Source: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03−044.asp

29. *October 15, Microsoft* — **Microsoft Security Bulletin MS03−045: Buffer Overrun in the ListBox and in the ComboBox Control Could Allow Code Execution .** The ListBox control and the ComboBox control both call a function, which is located in the User32.dll file, that contains a buffer overrun. The function does not correctly validate the parameters that are sent from a specially−crafted Windows message. **An attacker who had the ability to log on to a system interactively could run a program that could send a specially−crafted Windows message to any applications that have implemented the ListBox control or the ComboBox control, causing the application to take any action an attacker specified**. This could give an attacker complete control over the system by using Utility Manager in Windows 2000. **Microsoft has assigned a risk rating of "Important" to this issue** and recommends that system administrators install the patch immediately.
Source: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03−045.asp

30. *October 15, Microsoft* — **Microsoft Security Bulletin MS03−046: Vulnerability in Exchange Server Could Allow Arbitrary Code Execution. In Exchange Server 5.5, a vulnerability exists in the Internet Mail Service that could allow an unauthenticated attacker to connect to the SMTP port on an Exchange server and issue a specially−crafted extended verb request that could allocate a large amount of memory**. This could shut down the Internet Mail Service or could cause the server to stop responding because of a low memory condition. **In Exchange 2000 Server, a vulnerability exists that could allow an unauthenticated attacker to connect to the SMTP port on an Exchange server and issue a specially−crafted extended verb request**. That request could cause a denial of service that is similar to the one that could occur on Exchange 5.5. Additionally, if an attacker issues the request with carefully chosen data, the attacker could cause a buffer overrun that could allow the attacker to run malicious programs of their choice in the security context of the SMTP service. **Microsoft has assigned a risk rating of "Critical" to this issue** and recommends that system administrators install the patch to Exchange servers immediately.
Source: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03−046.asp

31. *October 15, Microsoft* — **Microsoft Security Bulletin MS03−047: Vulnerability in Exchange Server 5.5 Outlook Web Access Could Allow Cross−Site Scripting Attack.** A cross−site scripting (XSS) vulnerability results due to the way that Outlook Web Access (OWA) performs HTML encoding in the Compose New Message form. **An attacker could seek to exploit this vulnerability by having a user run script on the attacker's behalf**. If the script executes in the security context of the user, the attacker's code could then execute by using the security settings of the OWA Web site (or of a Web site that is hosted on the same server as the OWA Web site) and could enable the attacker to access any data belonging to the site where the user has access. **Microsoft has assigned a risk rating of "Moderate" to this**

issue and recommends that system administrators install the patch immediately. **Users who have customized any of the ASP pages in the File Information section in this document should backup those files** before applying this patch as they will be overwritten when the patch is applied. A
Source: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03−047.asp

Internet Alert Dashboard

Current Alert Levels

AlertCon: 2 out of 4 https://gtoc.iss.net	Security Focus ThreatCon: 2 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_MSBLAST.A** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	135 (epmap), 1434 (ms−sql−m), 137 (netbios−ns), 445 (microsoft−ds), 1433 (ms−sql−s), 80 (www), 17300 (Kuang2TheVirus), 139 (netbios−ssn), 4662 (eDonkey2000), 27374 (SubSeven) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

32. *October 15, CNN* — **U.S. citizens advised to leave Gaza.** A bomb went off underneath a convoy carrying U.S. diplomats in Gaza on Wednesday, October 15, killing three American members of a security detail and injuring another. **The convoy, which was thought to be carrying twelve Americans, was in Gaza to interview Palestinian students who have applied for Fulbright scholarships in the United States**, U.S. Ambassador to Israel Daniel Kurtzer said. According to the State Department, **a roadside bomb was triggered immediately after the Palestinian police cars in the convoy passed by, hitting the U.S. vehicle**. No group has claimed responsibility. Several hours after the attack, the U.S. Embassy issued an advisory calling on U.S. citizens to leave Gaza. **The attack was believed to be the first aimed at Americans since the beginning of the current Palestinian uprising, now in its third year**. Kurtzer said the attack would not change the U.S. commitment to the peace process and the Palestinian Authority had been asked to arrest those responsible. Palestinian Prime Minister Ahmed Qorei strongly condemned the attack, offered his condolences, and promised an investigation.
Source: http://www.cnn.com/2003/WORLD/meast/10/15/mideast.blast/inde x.html

33. *October 15, Washington Times* — **Saudi protesters demand reforms.** Hundreds of Saudis marched down the main avenue of the capital, Riyadh, on Tuesday, October 14, in an unprecedented demonstration timed to coincide with the opening of the kingdom's first human rights conference. **The U.S., German and British embassies, meanwhile, warned the expatriate community on Tuesday, October 14, that there was credible evidence of a terrorist plot against the capital's two landmark skyscrapers. It was next to one of them, the Kingdom Tower, that demonstrators chanting "Allahu Akbar," or "God is Great," were dispersed by anti−riot police,** who fired shots into the air two hours after the protest began. Several demonstrators were arrested and taken away in buses, but witnesses said many were released after a few hours.
Source: http://www.washingtontimes.com/world/20031014−092554−5920r.h tm

34. *October 14, U.S. Department of State* — **Public Announcement: Djibouti. The U.S. Government has received indications of terrorist threats in the region aimed at U.S. and Western interests, including civil aviation**. All American citizens considering travel to Djibouti are advised to reevaluate their travel plans in light of the current situation. American citizens in Djibouti should remain vigilant, particularly in public places frequented by foreigners, such as hotels, restaurants and places of worship, and should also avoid demonstrations and large crowds.
Source: http://travel.state.gov/djibouti_announce.html

35. *October 13, Associated Press* — **Al Qaeda terrorists use migrant, drug routes.** The United States and other countries such as Syria, Iraq and Greece are pointing to growing evidence that al Qaeda operatives are increasingly using immigrant and drug−smuggling routes to sneak to the West. From the Middle East to the Rio Grande to Australia's tropical coast facing Asia, border patrols have been bolstered and captured illegal immigrants are being increasingly evaluated for possible terrorist ties. **Experts wonder if this could just be the beginning as terrorists seek a back door around even the most seamless security**. "In some ways, it's a perfect cover," said Saeed Laylaz, a security analyst in Teheran. "A terrorist pretends to be an economic migrant with no papers. Even if you're caught, you're usually just sent back and able to try again." Some experts believe the immigrant routes could be part of a reshaping of strategies by al Qaeda and other groups in response to worldwide security clampdowns. **Instead of hiding in plain sight−−as the September 11 hijackers managed to do−−terrorist cells may increasingly adopt underground tactics: no inspections at border points, no paper trail to track, the anonymity of the undocumented**. Some experts see an alliance of convenience developing between smugglers hungry for cash and terrorists willing to pay whatever it takes.
Source: http://straitstimes.asia1.com.sg/world/story/0,4386,214355,0 0.html

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631
Subscription and Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631 for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202−323−3204.

DHS/IAIP Disclaimer